

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224236

(43)Date of publication of application : 17.08.1999

(51)Int.Cl.

G06F 15/00
H04L 9/32

(21)Application number : 10-024225

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 05.02.1998

(72)Inventor : NAKAMURA HIROSHI
FUJII TERUKO
SADAKANE TETSUO
BABA YOSHIMASA

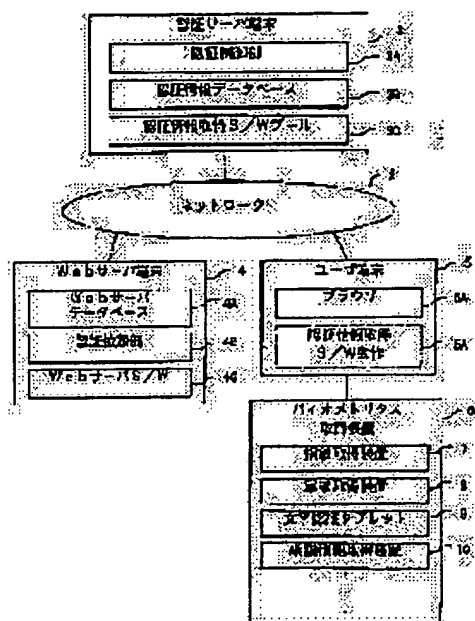
(54) REMOTE AUTHENTICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a remote authentication system capable of surely judging the identification an individual and the presence/absence of his access right and substantially improving handleability at the time of authenticating the individual by using obtained biometrics information and key inputted user identification information corresponding to the operation of a prescribed authentication information acquisition software.

SOLUTION: In a Web system 1, authentication is performed by biometrics information. In this case, corresponding to an accessing user terminal 5, a data kind as access information, an authentication request part 4B operated in a Web server terminal 4 as a client of the authentication, the environment of a Web server S/W4C being an application in use and authentication history (authentication time state), an authentication information obtaining S/W for dynamically obtaining the information required for the authentication is selected.

Thus, identification of an individual and the presence/absence of his access right are surely judged corresponding to the environment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-224236

(43) 公開日 平成11年(1999) 8月17日

(51) Int.Cl.⁸
G 0 6 F 15/00
H 0 4 L 9/32

識別記号
3 3 0

F I
G 0 6 F 15/00
H 0 4 L 9/00
3 3 0 F
6 7 3 D

審査請求 未請求 請求項の数 3 O L (全 14 頁)

(21) 出願番号 特願平10-24225
(22) 出願日 平成10年(1998) 2月5日

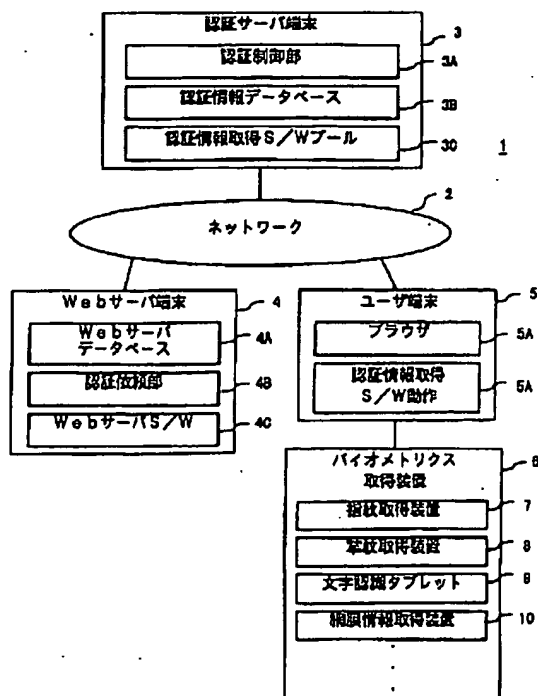
(71) 出願人 000006013
三菱電機株式会社
東京都千代田区丸の内二丁目2番3号
(72) 発明者 中村 浩
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内
(72) 発明者 藤井 照子
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内
(72) 発明者 貞包 哲男
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内
(74) 代理人 弁理士 宮田 金雄 (外2名)
最終頁に続く

(54) 【発明の名称】 遠隔認証システム

(57) 【要約】

【課題】 遠隔認証システムにおいて、バイオメトリクス情報によりユーザの認証を行う際、確実にユーザの特定とアクセス件の有無を判定し得ると共に使い勝手を格段的に向上する。

【解決手段】 ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、認証サーバにはユーザ端末及び又はユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して認証サーバからダウンロードされるユーザ端末及び又はユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにした。



果を実現できるが、表示では具体的に示されず予め決められた認証情報を送付する場合に、取得する手段がパスワード的な扱いとなるため、セキュリティを一段と向上できる。

【0050】なお上述の実施の形態1～4においては、Webサーバ端末4において、ユーザの個人認証を行う場合について述べたが、この発明はこれに限らず、例えばネットワークに接続された入退室端末装置等のように、ユーザの個人認証が必要な制御装置一般に広く適用できる。

【0051】

【発明の効果】上述の通りこの発明によれば、認証サーバは、バイオメトリクス情報により認証を行う際に、ユーザのバイオメトリクス情報の取得環境に応じて、バイオメトリクス取得装置と認証情報を自由に選択し取得するができ、かくして確実にユーザの特定とそのユーザのアクセス権の有無を判定し得る遠隔認証システムを実現できる。

【0052】またユーザは指定された認証情報の取得について不満があった場合に、取得する認証情報を変更や拒否することができ、バイオメトリクス取得装置が不潔等で不快感を伴う場合やバイオメトリクス情報を取得する装置が信頼できない場合でも、代替手段で確実にかくして確実にユーザの特定とそのユーザのアクセス権の有無を判定できる。

【図面の簡単な説明】

【図1】 この発明による遠隔認証システムを適用したWebシステムの実施の形態1の構成を示すブロック図である。

【図2】 図1のWebシステムにおける認証処理の説明に供するタイミングチャートである。

【図3】 図1の認証サーバ端末における認証情報データベースの実施例1の説明に供する図表である。

【図4】 図1の認証サーバ端末における認証情報データベースの実施例1の説明に供する図表である。

【図5】 図1の認証サーバ端末における認証情報データベースの実施例2の説明に供する図表である。

【図6】 図1の認証サーバ端末における認証情報データベースの実施例2の説明に供する図表である。

【図7】 図1の認証サーバ端末における認証情報データベースの実施例3の説明に供する図表である。

【図8】 図1のWebシステムにおける実施例3の認証処理の説明に供するタイミングチャートである。

【図9】 この発明による遠隔認証システムを適用したWebシステムの実施の形態2の構成を示すブロック図である。

10 【図10】 図9のWebシステムにおける認証処理の説明に供するタイミングチャートである。

【図11】 図1のWebシステムにおける認証処理の実施の形態3として拒否が発生した場合の説明に供するタイミングチャートである。

【図12】 図1のWebシステムの実施の形態4として認証情報取得S/Wの表示画面の説明に供する略線図である。

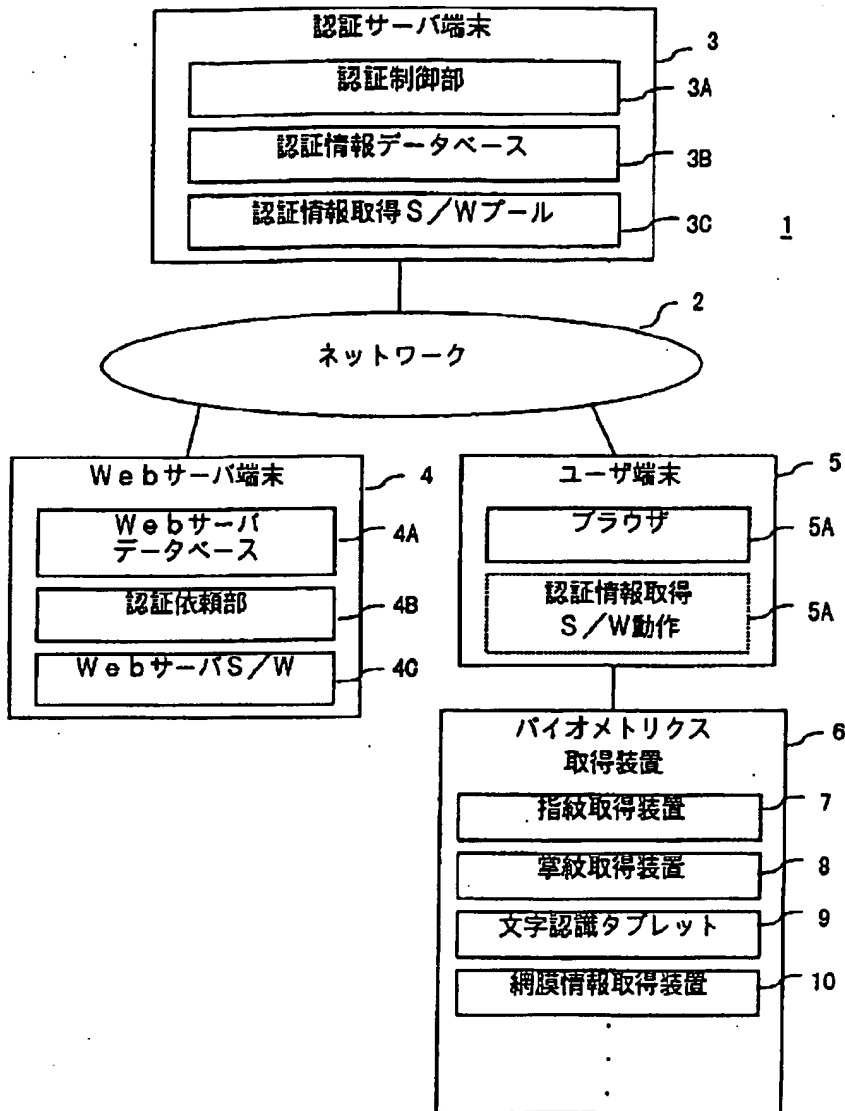
【符号の説明】

- 1 Webシステム
- 2 ネットワーク
- 3 認証サーバ端末
- 3A 認証制御部
- 3B 認証情報データベース
- 3C 認証情報取得ソフトウェアプール
- 4 Webサーバ端末
- 4A Webサーバデータベース
- 4B 認証依頼部
- 4C Webサーバソフトウェア
- 5 ユーザ端末
- 5A ブラウザ
- 5B 認証情報取得ソフトウェア動作
- 6 バイオメトリクス取得装置
- 7 指紋取得装置
- 8 掌紋取得装置
- 9 文字認識タブレット
- 10 網膜情報取得装置
- 11 認証情報取得ソフトウェア

【図3】

ユーザID	1 {名前、会社、社員番号、所属、住所、電話、など}	2
ユーザレベル	2			
認証情報	{指紋1、指紋2、筆跡、網膜、パスワード、ワンタイムパスワード情報}			

【図1】



【図4】

レベル	データ種別	認証情報取得S/W
1(最高機密)	1~10	A, B, C
2	11~20	D, E, F
3	21~30	G, H

A: 指紋と網膜
 B: 指紋2指
 C: 網膜と掌紋
 D: 指紋と掌紋
 E: 指紋
 F: 掌紋
 G: ワンタイムパスワード
 H: パスワード

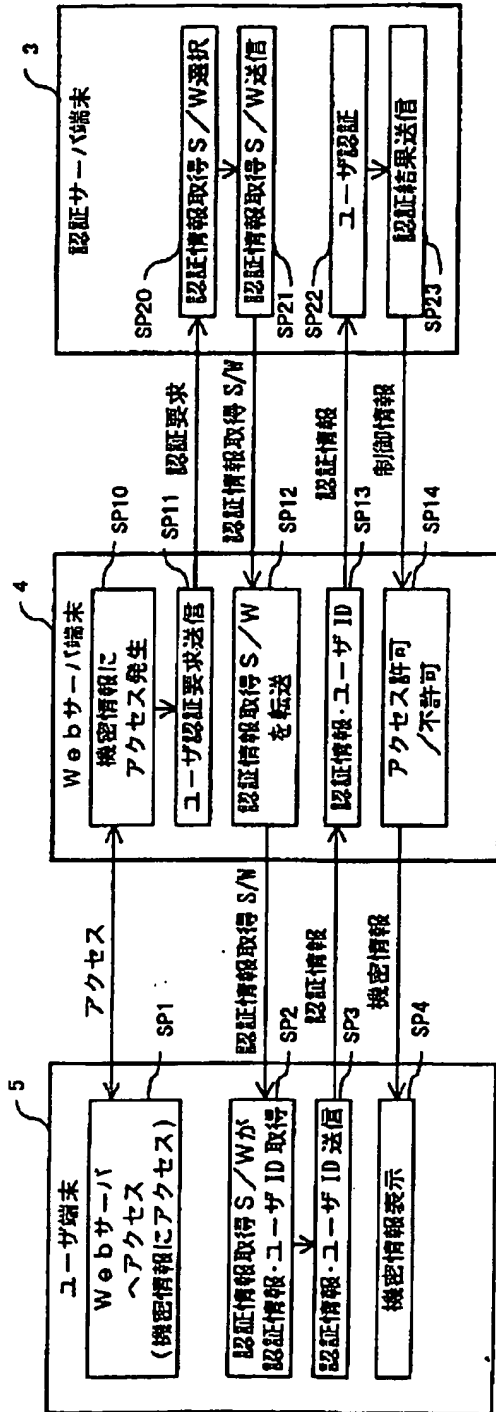
【図5】

認証クライアントID	認証情報取得S/W
	E, F
15	C, D, E
	A, B, C
	D, E, F
	G, H

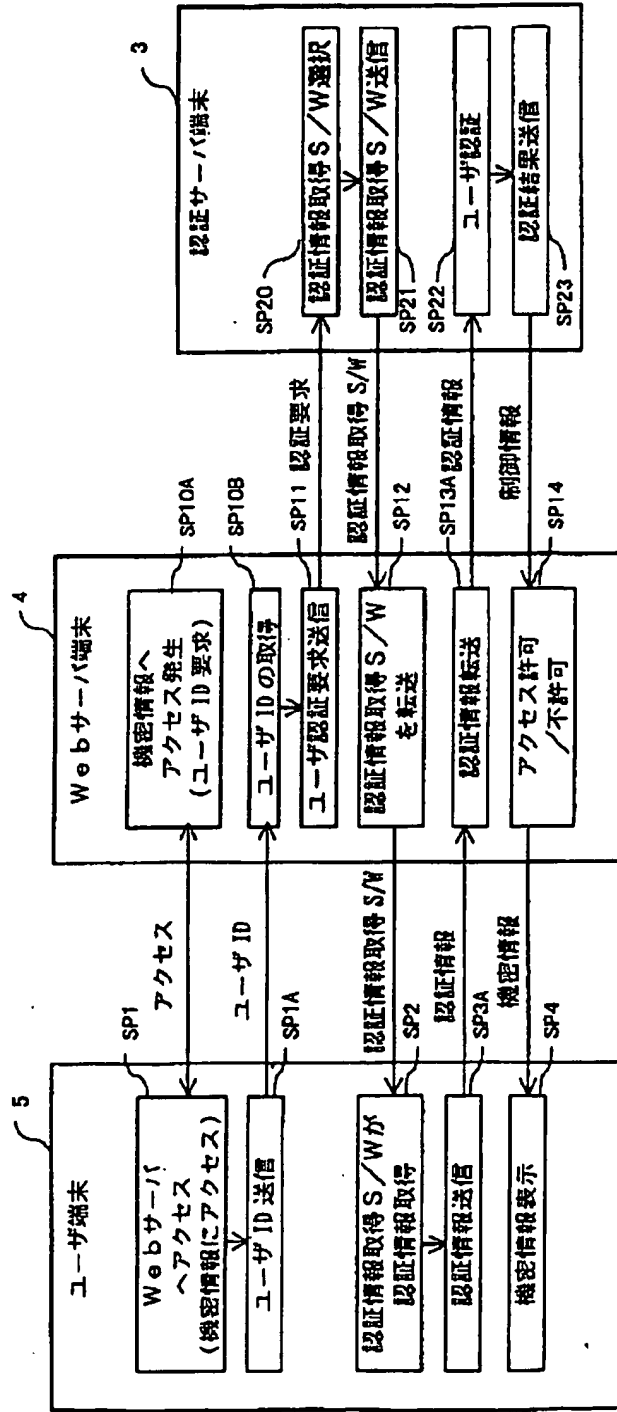
【図6】

アプリケーションID	認証情報取得S/W
	C, E, G
25	A, D, E, F
	E, F
	G, H

【図2】



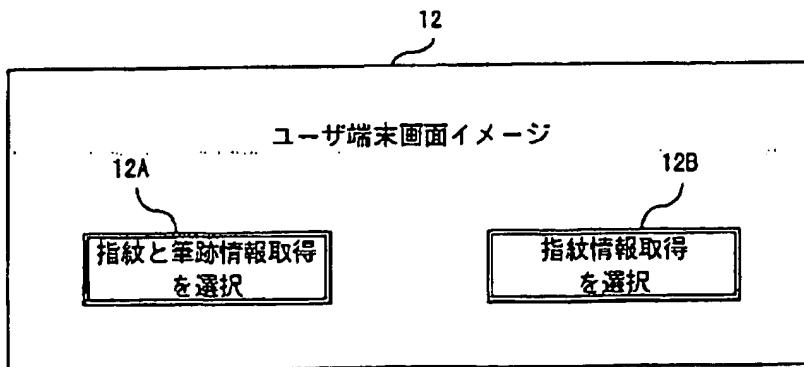
【図8】



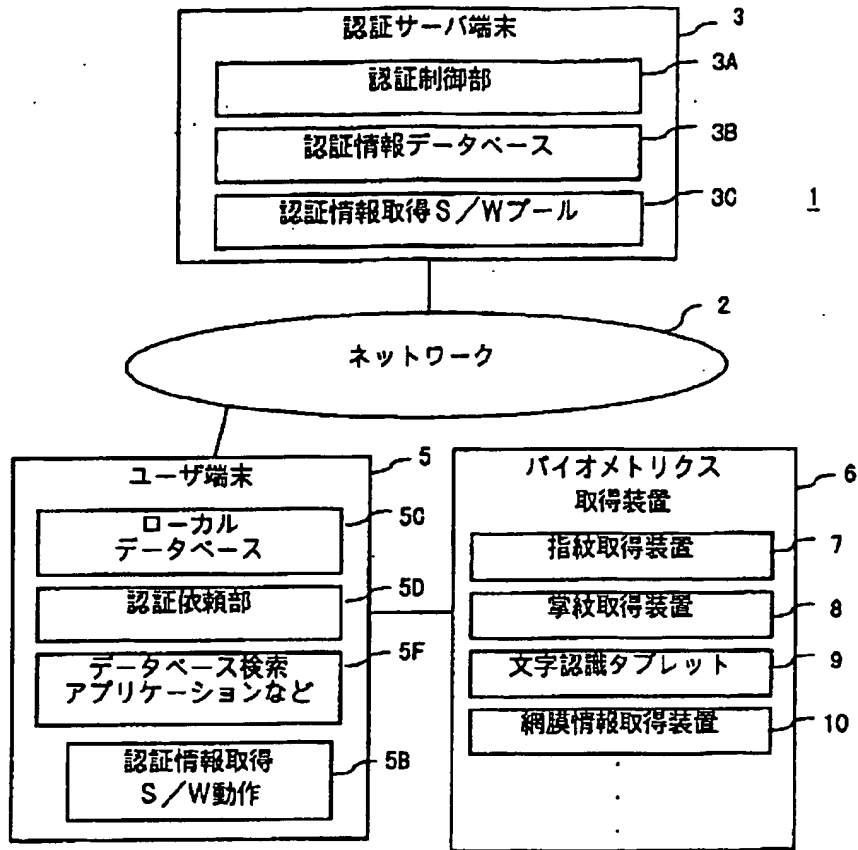
【図7】

ユーザ ID	1 {名前、会社、社員番号、所属、住所、電話、など}	2
ユーザ種別	一般			
ユーザレベル	2			
使用できるクライアント ID	10,15			
使用できるアプリケーション ID	8,25,36			
アプリケーション制御情報	key-1			
認証情報	{指紋 1、指紋 2、筆跡、網膜、パスワード、ワンタイムパスワード情報}			
照合ログ	前回 : 認証情報取得 S/W E 選択, 照合評価 90%, 指紋 1=90% 前々回 : 認証情報取得 S/W D 選択, 照合評価 75% 指紋 2=80%, 筆跡=70%			
総認証回数	20			
選択基準	総認証回数 (他例: 照合率)	.		

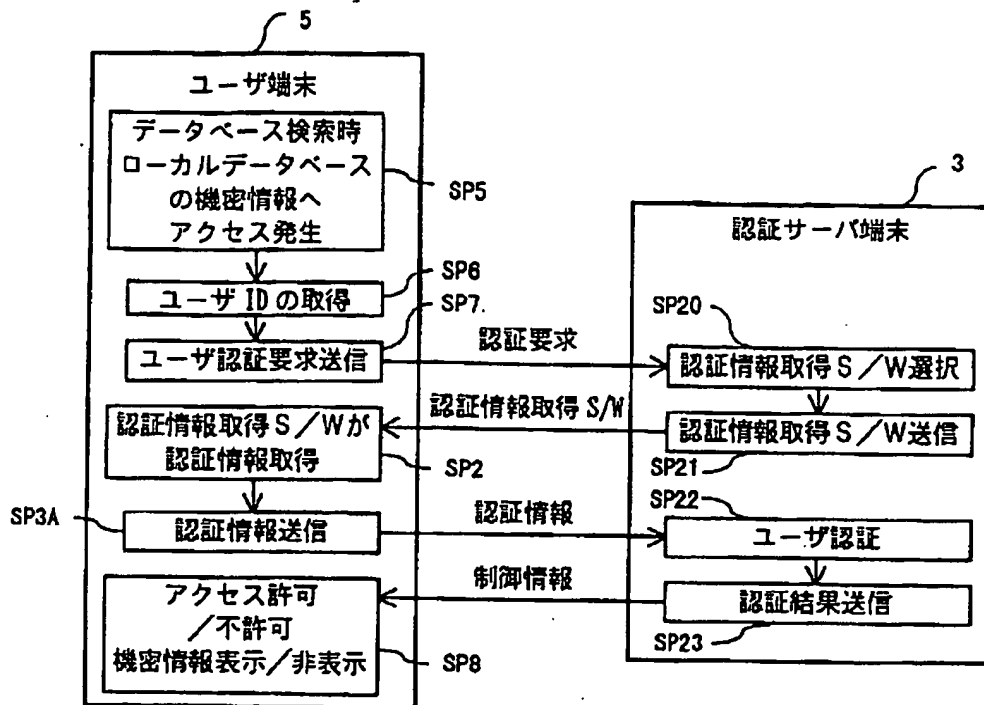
【図12】



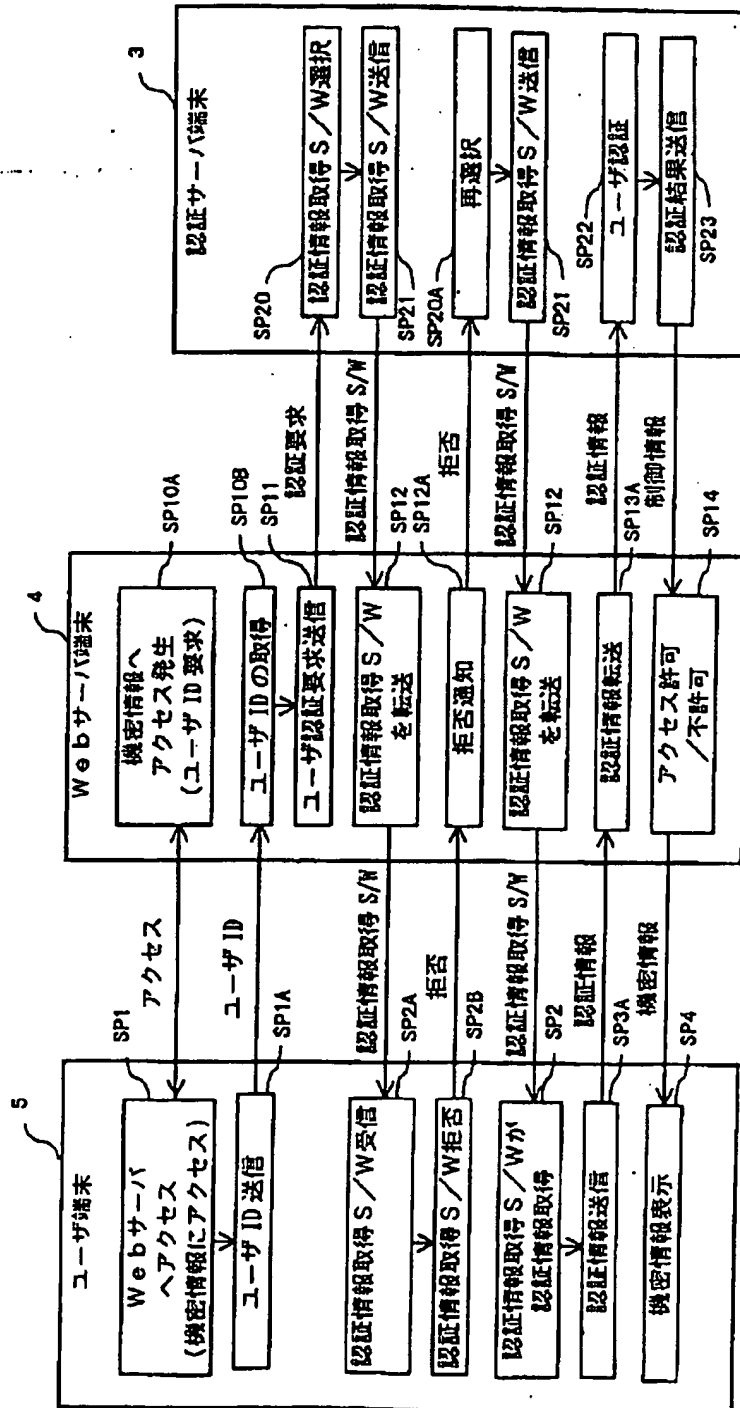
【図9】



【図10】



【図11】



フロントページの続き

(72)発明者 馬場 義昌

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内